(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-269288
(P2005-269288A)
(43)公開日　平成17年9月29日(2005.9.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/08	H04L 9/00	601C	5B085
G06F 15/00	G06F 15/00	330C	5J104
G09C 1/00	G09C 1/00	640E	
	H04L 9/00	601E	

審査請求 未請求　請求項の数 10　OL　（全 22 頁）

(21)出願番号　特願2004-79451(P2004-79451)
(22)出願日　平成16年3月19日(2004.3.19)

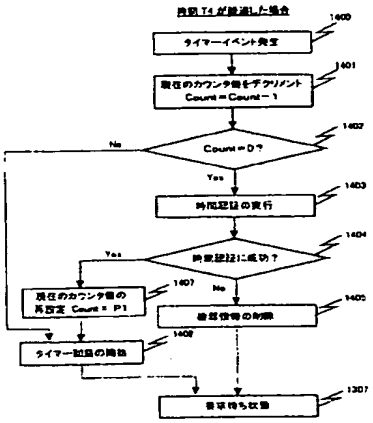
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(74)代理人　100100310
弁理士　井上　学
(72)発明者　大野　千代
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内
(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】コンテンツ送信装置、コンテンツ受信装置およびコンテンツ伝送方法

(57)【要約】
【課題】
有線または無線LANを用いてコンテンツの伝送を行う際に不正なコピーの作成を抑止して著作権の保護を図ると共に、コンテンツ伝送を個人の使用範囲を逸脱しないようにする。
【解決手段】
コンテンツ送信装置とコンテンツ受信装置は、コンテンツの伝送前に互いに認証を行う。この認証の際に、認証要求もしくは認証応答の送信に対する受信確認の到達までの時間を計測し、この値が一定の上限値を超えない場合に限り、暗号化したコンテンツ伝送を行うと共に、アドレス情報や装置固有の機器情報を登録し、再度コンテンツ伝送時には上記時間計測を行わないで暗号化したコンテンツ伝送を行う。また、定期的に上記時間計測を行い、上記登録情報を現状のネットワーク構成に適した内容になるように動的に管理する。
【選択図】　図１４

図14



【特許請求の範囲】
【請求項１】
ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うと共に、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該コンテンツ受信装置に対して認証要求あるいは時間確認要求を送信し該要求に対する応答を受信するまでの時間を計測するタイマー手段と、
該コンテンツ受信装置の機器情報を登録、管理する機器情報管理手段とを有し、
該機器情報管理手段は、該タイマー手段の測定結果が所定の値を超えない時、該コンテンツ受信装置のアドレス情報と装置固有の機器情報とを登録し、該登録した該コンテンツ受信装置に対して必要に応じて該タイマー手段による時間の計測を実行し、該測定結果に応じて該登録内容を制御することを特徴とするコンテンツ送信装置。
【請求項２】
ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、
該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うと共に、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、
該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、
該コンテンツ受信装置に対して認証要求あるいは時間確認要求を送信し、該要求に対する応答を受信するまでの時間を計測するタイマー手段と、
該コンテンツ受信装置の機器情報を登録、管理する機器情報管理手段とを有し、
該機器情報管理手段は、該タイマー手段の測定結果での測定結果が所定の値を超えない時、前記コンテンツ受信装置のアドレス情報と装置製造時に予め記憶させている装置固有の機器情報とを登録し、該登録した該コンテンツ受信装置に対して必要に応じて該タイマー手段による時間の計測を実行し、該測定結果に応じて該登録内容を制御することを特徴とするコンテンツ送信装置。
【請求項３】
前記コンテンツ受信装置からコンテンツ受信要求を受信した時、該機器情報管理手段に登録されたアドレス情報と装置固有の機器情報と、該コンテンツ受信装置のアドレス情報と装置固有の機器情報とが一致した場合、該タイマー手段による時間の計測を行わずに該コンテンツ受信装置へのコンテンツ送出を行うことを特徴とする請求項１または２のいずれかに記載のコンテンツ送信装置。
【請求項４】
前記機器情報管理手段に登録した前記コンテンツ受信装置に対して該タイマー手段による時間の計測を実行し、該タイマー手段の測定結果が所定の値を超えた時、該機器情報管理手段に登録した該コンテンツ受信装置に関するアドレス情報と装置固有の機器情報を削除することを特徴とする請求項１または２のいずれかに記載のコンテンツ送信装置。
【請求項５】
前記機器情報管理手段に登録した前記コンテンツ受信装置に対して、所定の時間毎あるいは所定のコンテンツパケット数毎に、該タイマー手段を用いて時間の計測を行い、該タイマー手段の測定結果に応じて該機器情報管理手段に登録した内容を更新することを特徴とする請求項１から３のいずれかに記載のコンテンツ送信装置。
【請求項６】
前記機器情報管理手段に登録したコンテンツ受信装置に対して、電源投入時、システム起動時またはネットワーク接続時に、該タイマー手段を用いて時間の計測を行い、該タイマー手段の測定結果に応じて該機器情報管理手段に登録した内容を更新することを特徴とする請求項１から３のいずれかに記載のコンテンツ送信装置。
【請求項７】

前記機器情報管理手段に登録したコンテンツ送信先のコンテンツ受信装置に対して、コンテンツの予約実行時やコンテンツの内容が変化した時に、該タイマー手段を用いて時間の計測を行い、該タイマー手段の測定結果に応じて該機器情報管理手段に登録した内容を更新することを特徴とする請求項１から３のいずれかに記載のコンテンツ送信装置。

【請求項８】

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

該ネットワークを介して接続されるコンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、

該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置からの認証要求に対する認証の判定を行う認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの復号化処理を行う復号化手段とを有し、

該コンテンツ送信装置から送信された時間確認要求に対して応答し、該コンテンツ送信装置において該応答までの時間を計測され、該コンテンツ送信装置に対して必要に応じて、コンテンツ送信装置からの該時間確認要求の送信を要求することを有することを特徴とするコンテンツ受信装置。

【請求項９】

該コンテンツ送信装置から送信された時間確認要求に対して応答し、該コンテンツ送信装置において該応答までの時間を計測され、該計測結果が所定の値を超えない時、自身のアドレス情報と装置固有の機器情報とを該コンテンツ送信装置に登録され、

該コンテンツ送信装置に対して時間確認要求の送信を要求し、該コンテンツ送信装置から送信された時間確認要求に対して応答し、該コンテンツ送信装置において該応答までの時間を計測され、該計測結果に応じて該登録された内容が更新されることを特徴とする請求項８記載のコンテンツ受信装置。

【請求項１０】

ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信するコンテンツ送信装置におけるコンテンツ伝送方法であって、

該コンテンツ受信装置にコンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うと共に、該コンテンツ受信装置に対して自身の認証要求を発行するステップと、

該コンテンツ受信装置に対して認証要求あるいは時間確認要求を送信し該要求に対する応答を受信するまでの時間を計測するステップと、

該コンテンツ受信装置の機器情報を登録、管理するステップと、

該機器情報を登録、管理する際、該時間を計測するステップにおける測定結果が所定の値を超えない時、前記コンテンツ受信装置のアドレス情報と装置固有の機器情報とを登録するステップと、

該登録した該コンテンツ受信装置に対して必要に応じて該時間を計測するステップを実行し、該計測した測定結果に応じて該登録内容を制御するステップとを有することを特徴とするコンテンツ伝送方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、映像音声等のコンテンツをネットワークを介して送受信するのに際して、伝送されるコンテンツの著作権を保護するのに好適な送信装置、受信装置に関する。

【背景技術】

【０００２】

パーソナルコンピュータ（以下PCと記す）の演算速度や記憶容量など処理能力の発展に伴い、PCに内蔵されるハードディスクドライブ（以下HDDと記す）も大容量化が進んでいる。こうした状況のもとで最近では一般の家庭で利用されるようなランクのPCにおいてもHDDを利用してTV放送番組を録画し、これをPCのディスプレイで視聴を行うといった使い

方ができるようになってきた。またその一方では大容量HDDの低価格化により、家庭用の録画装置としてもHDDを内蔵してこれに映像音声情報をデジタル記録するようなHDD録画装置が登場してきており、ディスクを録画媒体として使うことに拠る使い勝手の良さが着目されている。

【０００３】

一方コンテンツ等の情報の著作権保護のため、デジタルＡＶ機器に取り入れられているコピープロテクトの方法の一例として例えばＩＥＥＥ１３９４バス上でのコピープロテクト方法を定めたＤｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ（ＤＴＣＰ）方式がある（非特許文献１に記載）。

そして、装置間、あるいはネットワーク間での著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば特許文献１、特許文献２に開示されている。

【０００４】

【特許文献１】特開２０００－２８７１９２号公報

【特許文献２】特開２００１－３５８７０６号公報

【非特許文献１】Ｈｉｔａｃｈｉ，Ｌｔｄ．他、５Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｗｈｉｔｅ Ｐａｐｅｒ

【発明の開示】

【発明が解決しようとする課題】

【０００５】

上記したようなHDDを利用した録画装置やPCなどでは映像音声情報は装置内に固定されたHDDに録画されているため、家の中の他の部屋で録画した番組を視聴しようとするような場合には装置自体を持ち運ぶしかなく、VTRなど取替え可能な媒体を利用する録画再生装置を複数備えて行えるような、媒体レベルでの映像音声情報の持ち運びは実現が難しかった。

そこで、このような録画装置に有線あるいは無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のインターフェースを搭載して、ネットワークを介して他のＰＣあるいは受信装置に送信することにより、宅内のどこでも録画された映像音声情報を視聴できるようにすることが考えらる。

【０００６】

家庭用の録画装置に有線あるいは無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のインターフェースを搭載して、コンテンツをネットワークを介して他のＰＣあるいは受信装置に送信して、宅内のどこでも録画された映像音声情報を視聴できるようにする場合従来は、著作権を保護すべき映像音声情報（以下コンテンツとして説明する）の著作権保護については配慮がされておらず、ＨＤＤに録画されている映像音声情報は、ＬＡＮを介して受信した他のＰＣにおいて更にＨＤＤに保存することが可能であり、扱える映像音声情報はコピーが自由に行える「Copy free」のコンテンツでなければならなかった。

【０００７】

一般にデジタル録画されたコンテンツを上記のようにネットワーク等を介してある装置から他の装置へ伝送して記録を行うような場合には伝送時のデータ品質の劣化が少なく、送信側の装置にあるコンテンツと同じ品質のコピー（複製）が受信側で作成できるため、著作権を保護すべき映像および音声データ（以下コンテンツと呼ぶ）に対しては、個人的利用の範囲を逸脱したコンテンツの不正なコピー作成を防止できるような配慮が必要である。例えばデジタルＡＶ機器の間でコンテンツを送信する際には、コンテンツ送信装置側において暗号化を行い、コンテンツ受信装置側との間で復号化のための情報の共有化を行うことによって、送信先であるコンテンツ受信装置以外の機器によってコンテンツが正しく受信されて復号されない様にして、無制限なコピーの作成を防ぐコピープロテクトが実施されている。

【０００８】

このようなコピープロテクトの方法の一例としてデジタルＡＶ機器に取り入れられてい

るものには、例えば非特許文献１に記載されているＤＴＣＰ方式がある。ＤＴＣＰ方式ではコンテンツを「Copy free」「Copy one generation」「No more copies」「Copy never」に分類して管理し、録画装置では「Copy free」「Copy one generation」のコンテンツだけを記録し、「Copy one generation」のコンテンツは一度記録した後は「No more copies」として取り扱い、バス上では「Copy free」のコンテンツを除いて送信側で暗号化処理を施して伝送を行うことによって、無制限なコンテンツのコピーが行えないようにしている。

【０００９】

有線あるいは無線のＬＡＮによるコンテンツ伝送においても、ＤＴＣＰ方式と同様な考え方により、著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば特許文献１は、ネットワーク上のデジタルコンテンツ流通のためのコピープロテクトの方式にＤＴＣＰと同様の手法を適用するための技術が開示されており、特許文献２にも同様にコンテンツを著作権保護のために暗号化して通信する装置間を構成するための技術が開示されている。

そして、これらはコンテンツを有線あるいは無線ＬＡＮを介して伝送する際には、送信側と受信側が同じ家の中に有るかどうかは考慮していない。むしろ、配信サーバからダウンロードを行うような場合には、送信側はプロバイダのサイトに有り、受信側は一般家庭などに有ることが普通である。

【００１０】

したがってＰＣのＨＤＤやＨＤＤを内蔵した録画装置でコンテンツを録画して、ここから宅内の他の装置にＬＡＮを介した伝送を行おうとする場合に上記の技術を適用したとしても、宅内のＬＡＮがインターネットに接続されているとインターネットを介して接続される他の宅内に置かれている受信装置でコンテンツを受信して表示することができ、しかもその範囲はインターネットに接続されていれば世界中のあらゆる場所に広がることになる。

このような状況では、例え上記したような技術でコピープロテクトを行おうとしても、録画装置の使用者がこの録画装置をインターネットからアクセス可能な状態にすることによって、上記のコピープロテクトを備えた受信装置であれば自由にコンテンツを受信して表示することができ、本来の著作権保護の目的である個人的利用の範囲を大きく逸脱することになってしまう。

【００１１】

本発明の目的は、宅内の有線または無線のＬＡＮを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に制限することのできるコンテンツ或いは情報送信装置、受信装置およびコンテンツ伝送方法を提供することにある。

【課題を解決するための手段】

【００１２】

上記の課題を解決するために本発明では、ネットワークを介してコンテンツの送信を行うコンテンツ送信装置において、ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、該ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うと共に、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、該コンテンツ受信装置への認証要求あるいは時間確認要求を送信し、該要求に対する応答を受信するまでの時間を必要に応じて計測する、もしくは該コンテンツ受信装置からの認証要求に対する応答の送信に対する該コンテンツ受信装置からの受信確認の到達までの時間を必要に応じて計測するタイマー手段（時間計測手段）と、該コンテンツ受信装置の機器情報を登録および管理、チェックする機器情報管理手段とを有し、

該機器情報管理手段は、該タイマー手段の測定結果に応じて該コンテンツ受信装置のアドレス情報と装置製造時に予め記憶させている装置固有の機器情報の登録を制御するようにする。

また、前記タイマー手段において、該タイマー手段の測定結果が所定の値を超えない時、前記コンテンツ受信装置のアドレス情報と装置固有の機器情報を前記機器情報管理手段に登録するようにする。

【００１３】

また、上記コンテンツ受信装置からコンテンツ受信要求を受信した時、該機器情報管理手段に登録されたアドレス情報と装置固有の機器情報と、該コンテンツ受信装置のアドレス情報と装置固有の機器情報とを比較しこれらが一致した場合、該タイマー手段による時間の計測を行わずに該コンテンツ受信装置へのコンテンツ送出を行うようにする。

また、上記コンテンツ受信装置に関する登録情報を適切に管理するために、該情報を登録した該コンテンツ受信装置に対して、定期的にあるいは任意のタイミングで該タイマー手段による時間の計測を行い、該測定結果に応じて該登録情報を更新するようにする。

【００１４】

更に、上記課題を解決するため本発明では、ネットワークを介してコンテンツを受信するコンテンツ受信装置において、ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、該ネットワークを介して接続されるコンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、

該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置からの認証要求に対する認証の判定を行う認証手段と、該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段と、該コンテンツ送信装置への認証要求の送信もしくは該コンテンツ送信装置からの認証要求に対する応答の送信に対する該コンテンツ送信装置からの受信確認の到達までの時間を計測するタイマー手段、もしくは該コンテンツ送信装置に対して時間確認要求の送信を要求し、該コンテンツ送信装置から送信された時間確認要求に対して応答する手段と、該コンテンツ送信装置の機器情報を登録、管理する機器情報管理手段とを有し、該機器情報管理手段は、該タイマー手段の測定結果に応じて該コンテンツ送信装置のアドレス情報と装置製造時に予め記憶させている装置固有の機器情報の登録を制御するようにする。

【００１５】

また、上記コンテンツ送信装置に関する登録情報を適切に管理するために、該情報を登録した該コンテンツ送信装置に対して、定期的にあるいは任意のタイミングで該タイマー手段による時間の計測を行い、該測定結果に応じて該登録情報を更新するようにする。

また該コンテンツ送信装置から送信された時間確認要求に対して応答し、該コンテンツ送信装置において該応答までの時間を計測され、該計測結果が所定の値を超えない時、自身のアドレス情報と装置固有の機器情報とを該コンテンツ送信装置に登録され、

該コンテンツ送信装置に対して必要に応じて時間確認要求の送信を要求し、該コンテンツ送信装置から送信された時間確認要求に対して応答し、該コンテンツ送信装置において該応答までの時間を計測され、該計測結果に応じて該登録された内容が更新されるようにする。

【００１６】

すなわち、本発明では、コンテンツ送信装置とコンテンツ受信装置はコンテンツの伝送を行う前に、お互いの認証を行いこの認証の際に、認証要求もしくは認証応答の送信に対する受信確認の到達までの時間を計測して、この値が一定の上限値を超えない場合に限り、共有化した鍵データによって暗号化されたコンテンツの伝送を行うと共に、アドレス情報と装置固有の機器情報を登録して、再度コンテンツ伝送時には上記時間計測を行わないで暗号化されたコンテンツを伝送するようにする。また、定期的にあるいは任意のタイミングでアドレス情報と装置固有の機器情報の内容を見直しし、ネットワークに未接続の装置や使用頻度の低い装置が登録されたままにならないようにする。

これにより、宅内の有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの不当な視聴や複製の作成を個人的利用の範囲に制限することができる。

【発明の効果】

【００１７】

本発明によれば、宅内の有線または無線のLANを利用したコンテンツ送信装置、受信装置およびコンテンツ伝送の信頼性向上を図ることができる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明の実施の形態について図面を用いて説明する。

【実施例１】

【００１９】

以下本発明の実施例１について説明する。

図１は本発明の一実施形態であるコンテンツ送信装置１００およびコンテンツ受信装置２００の構成を示したものであり、コンテンツ送信装置１００とコンテンツ受信装置２００とは互いにLANを介して接続されている。コンテンツ送信装置１００において、１０１はコンテンツ送信装置２００にコンテンツを送り出すコンテンツ送信回路、１０２はコンテンツ送信回路１０１の出力するコンテンツを暗号化する暗号化回路、１０３は暗号化回路１０２の出力および認証回路１０４の入出力をLANを介して他の装置とやり取りするネットワーク通信処理回路、１０４はLAN上に接続される他の装置との間で情報をやり取りして装置間の相互認証を行なう認証回路、１０５は認証回路１０４での処理に必要な情報を蓄える不揮発メモリ、１０６は認証回路１０４の情報に基づき暗号化回路１０２でコンテンツ暗号化のために必要な鍵情報を生成する鍵生成回路、１０７は認証回路１０４が発生する認証要求などの情報を他の装置に送信してから該情報に対する受信確認が到達するまでの時間を測定するタイマー回路、１０８は認証回路１０４で認証した他装置の機器情報を登録し、これを管理する機器情報登録回路であり、コンテンツ送信回路１０１から送信されるコンテンツにはその取り扱い方を示す「Copy free」「Copy one generation」「No more copies」「Copy never」の識別コードを付してコンテンツ受信装置に送信される。

【００２０】

コンテンツ受信装置２００において、２０１はLANを介して送られてきたコンテンツを受信するコンテンツ受信回路、２０２はコンテンツ送信回路１００の暗号化回路１０２で暗号化されたコンテンツをネットワーク通信処理回路２０３から受け取り複合化してコンテンツ受信回路２０１に出力する複合化回路、２０３は他の装置との間でネットワークを介して複合化回路２０２への入力および認証回路２０４の入出力をやり取りするネットワーク通信処理回路、２０４は他の装置との間で情報をやり取りして装置間の相互認証を行う認証回路、２０５は認証回路２０４での処理に必要な情報を蓄える不揮発メモリ、２０６は認証回路２０４の出力する情報に基づき複合化回路２０２でのコンテンツ複合化のために必要な鍵を生成する鍵生成回路、２０７は認証回路２０４から他の装置に認証要求などの情報を送信してから該情報に対する受信確認が到達するまでの時間を測定するタイマー回路、２０８は認証回路２０４で認証した他装置の機器情報を登録し、これを管理する機器情報登録回路からなり、受信したコンテンツは該コンテンツと共に送信される「Copy free」「Copy one generation」「No more copies」「Copy never」の識別コードに従って処理され、「Copy free」「Copy one generation」のコンテンツ記録媒体への記録が可能であり、「Copy one generation」のコンテンツを記録した場合にはそれ以後該コンテンツは「No more copies」として取り扱う。

【００２１】

図２は、コンテンツ送信装置１００およびコンテンツ受信装置２００を含む宅内LANの構成例を示したものである。１台のコンテンツ送信装置１００と２台のコンテンツ受信装置２００ａ、２００ｂは有線LANのケーブルによりネットワークハブ装置３００にそれぞ

れ接続され、ネットワークハブ装置３００はルータ４００に接続される。ルータ４００はモデムや光電変換器などを介してインターネットへ接続される。上記コンテンツ送信装置１００、およびコンテンツ受信装置２００ａ、ｂ、ルータ４００はそれぞれLAN上で自身を識別するIPアドレスを所有する。また各々のネットワーク通信処理回路のインターフェース部には４８ビットのMAC（Media Access Control）アドレスが予め製造時に与えられている。各装置へのIPアドレスの設定は、従来よりネットワークにおけるアドレスの自動設定に広く採用されているDHCP（Dynamic Host Configuration Protocol）により、例えばルータ４００をDHCPサーバとして動作させ、ここから各装置のIPアドレスを割り振るようにすれば良い。なお、IPv6（Internet Protocol Version 6）を用いる場合にはステートレス自動設定と呼ばれる方法によりルータ４００のIPアドレスの上位６４ビットとMACアドレスから各装置が自身のIPアドレスを定めることも可能である。

【００２２】

図３はコンテンツ送信装置１００が保持する機器情報登録手段１０８の構成を示した図である。例えば、コンテンツ送信装置１００が接続されているネットワークにコンテンツ受信装置２００が接続された場合のコンテンツ受信装置２００のアドレス情報と装置固有の機器情報の登録方法の一例を説明する。１０８１はコンテンツ受信装置２００からアドレス情報や装置固有の機器情報を取得する機器情報取得部、１０８２は該機器情報取得部１０８１で取得したコンテンツ受信装置２００のアドレス情報や装置固有の機器情報を登録しておく機器情報登録部、１０８３はコンテンツ受信装置の登録や、機器情報登録部１０８２に登録された機器情報からコンテンツ受信装置２００を認証する機器情報管理部である。機器情報取得部１０８１において、コンテンツ受信装置２００へ向けて、例えば機器情報登録用アプリケーションあるいはブラウザを用いた登録用のWebページを送信する。該機器情報登録用アプリケーションあるいは登録用Webページを受信したコンテンツ受信装置２００は、機器情報登録用アプリケーションあるいは登録用Webページの指示内容に従って、自動的にまたはユーザによる登録項目の入力により、自身のアドレス情報や装置固有の機器情報をコンテンツ送信装置１００に登録する。ここで、上記装置固有の機器情報は、例えば特定の認証機関により生成されコンテンツ受信装置２００の不揮発メモリ２０５に保存されている公開鍵である。該公開鍵は、コンテンツ受信装置２００の製造時に予め不揮発メモリ２０５に記憶されている公開鍵であるので、装置毎にユニークな値を持つ。図４は、機器情報登録部１０８２に登録される機器情報の一例である。コンテンツ受信装置２００のアドレス情報としてIPアドレスとMACアドレスを、装置固有情報として該コンテンツ受信装置２００の不揮発メモリ２０５に保存されている公開鍵を登録している。

【００２３】

以上のことから、コンテンツ送信装置１００は、コンテンツ受信装置２００を認証する時に、上記機器情報登録手段１０８に登録されている機器情報を元に、登録されたコンテンツ受信装置２００を特定することが可能となる。

ここで、装置固有情報として、ネットワークを介して接続されるコンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送にコピープロテクト方法を定めたDTCPを用いた時、お互いを認証する際に使用する公開鍵を例にとって説明しているが、特に公開鍵に限定されるものではなく、装置を特定可能なユニークな情報を登録するようにする。

また本実施例１では、コンテンツ送信装置１００がコンテンツ受信装置２００の機器情報を登録する方法について述べたが、コンテンツ受信装置２００がコンテンツ送信装置１００を登録する方法についても上記説明通りである。

【実施例２】

【００２４】

次に本発明の実施例２について以下説明する。

本実施の形態の特徴は、有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に限定することのできるコンテン

ツ送信装置、受信装置を提供することが可能となる。

【００２５】

図５はコンテンツ送信装置１００とコンテンツ受信装置２００によるコンテンツ送受信の際の手順の一例を示したものである。左側がコンテンツ送信装置１００を、右側がコンテンツ受信装置２００を表しており、両者の間の情報の送受信のタイミングと方向を矢印により示している。

始めにコンテンツ受信装置２００側から認証要求を作成する。認証要求には前記した装置固有の公開鍵と、該公開鍵に対する証書を付してコンテンツ送信装置１００に送る。認証要求を受け取りその受信確認をコンテンツ受信装置２００に送ると、コンテンツ送信装置１００は自分の側からの認証要求を作成し、コンテンツ受信装置の場合と同様に認証機関が発行したコンテンツ送信装置１００の固有の公開鍵とその証書を付してコンテンツ受信装置２００に送り、タイマー回路１０７をスタートさせ、認証要求に対する受信確認がコンテンツ受信装置２００から受信されるまでの時間Ｔ１を測定する。タイマー回路１０７での計測値が所定の値（Ｔ）を超えない場合、すなわちＴ１＜Ｔである時、コンテンツ受信装置２００は個人的利用の範囲内に存在する装置であることを認証（以下、時間認証と呼ぶ）する。

【００２６】

この時、上記コンテンツ受信装置２００側から認証要求をコンテンツ送信装置１００へ送信する時、タイマー回路２０７をスタートさせ、コンテンツ送信装置１００からの受信確認が受信されるまでの時間Ｔ２を測定することで、時間認証を行うことも可能である。以上のようにして相互に認証に成功すると互いに共通の認証鍵が生成されて共有される。上記認証鍵の生成には周知の鍵交換アルゴリズムを利用すればよい。認証鍵の共有が完了するとコンテンツ送信装置１００は交換鍵と乱数を生成し、交換鍵と乱数をそれぞれ認証鍵により暗号化してコンテンツ受信装置２００に送る。

なお、図５では交換鍵と乱数を別々にコンテンツ送信装置１００からコンテンツ受信装置２００に送信しているがこれらをまとめて送るようにしてもよい。コンテンツ受信装置２００では認証鍵を用いてコンテンツ送信装置１００から送信された交換鍵を復号し、同様に受信して復号した乱数と共に保有する。続いてコンテンツ送信装置１００およびコンテンツ受信装置２００各々の側で交換鍵と乱数を用いて予め定められた計算アルゴリズムに従い共通鍵を生成する。このようにして得た共通鍵によってコンテンツ送信装置１００からコンテンツを暗号化して送信し、コンテンツ受信装置２００では復号化されたコンテンツを受信することができるようになる。

【００２７】

コンテンツ送信装置１００とコンテンツ受信装置２００間で認証が成功した場合、コンテンツ受信装置２００はコンテンツ送信装置１００へ向けてコンテンツ送信要求が送られ、これをきっかけに暗号化されたコンテンツの送信を行うようにする。必要なコンテンツの送信が完了したらコンテンツ送信装置１００は認証鍵、交換鍵、コンテンツの暗号化と復号化に必要な共通鍵を破棄する。コンテンツ受信装置２００においても上記同様に認証鍵、交換鍵、共通鍵を破棄し、再度コンテンツの受信を行おうとする際には新たに認証要求から行えば良いが、本発明の実施の形態ではコンテンツ受信装置２００が時間認証された時、前記したようにコンテンツ送信装置１００の機器情報登録回路１０８にコンテンツ受信装置２００のアドレス情報と装置固有の機器情報が登録される。これにより、コンテンツ送信装置１００の機器情報登録回路１０８に登録されたコンテンツ受信装置２００に対して、コンテンツ送信装置１００とコンテンツ受信装置２００は上記共通鍵を破棄せずに保持することで、再度コンテンツの受信を行う際、新たに認証要求から行う必要はない。

【００２８】

図６は上記した時間認証において、更にセキュアにかつ正確な時間が測定できる一例を示したものである。図６に示すようにコンテンツ送信装置１００とコンテンツ受信装置２００間で認証が成功し、互いに共通のコンテンツ送信装置１００はコンテンツ受信装置２

００へ向けて宅内確認要求を送信すると同時にタイマー回路１０７をスタートさせる。コンテンツ受信装置２００は、上記コンテンツ送信装置１００からの宅内確認要求に対する受信確認をコンテンツ送信装置１００へ送信後、宅内確認応答を送信する。コンテンツ送信装置１００は、コンテンツ受信装置２００から宅内確認応答を受信した時までの時間Ｔ３を測定し、Ｔ３が所定の値を超えない場合を宅内に存在する受信装置として認証する。このように、コンテンツ送信装置１００とコンテンツ受信装置２００とで機器間の認証を行い、お互いに認証を行った後に、上記時間認証を行うことで、よりセキュアでかつ正確な時間認証を行うことができるようになる。

【００２９】

コンテンツ送信装置１００からコンテンツ受信装置２００にコンテンツを送信するのに使用するプロトコルは特定のものに限定されることはなく、RTP（Real-time Transport Protocol）、HTTP（Hyper Text Transfer Protocol）、FTP（File Transfer Protocol）等を用いることが可能である。コンテンツの伝送に際しては各転送プロトコルにおけるペイロード部分に共通鍵を用いて予め決められたアルゴリズムにより暗号化したコンテンツを収容して送信すれば良い。暗号化アルゴリズムとしては例えば周知の暗号化技術であるAES（Advanced Encryption Standard）を使用すれば良い。

以上のことから本発明の第２の実施の形態において、コンテンツ送信装置は一度時間認証されたコンテンツ受信装置のアドレス情報と装置固有の機器情報をコンテンツ送信装置が登録し、再度コンテンツの受信を行なう際、コンテンツ受信装置の時間認証を行なうことなく、暗号化されたコンテンツを送信することができ、コンテンツの受信毎に行なっていた時間認証を省略することができる。

【実施例３】

【００３０】

以下本発明の実施例３について説明する。

また、本発明の実施例３によると、例えば携帯端末によりインターネットを介してコンテンツ送信装置１００からコンテンツ視聴も可能となる。

図７はインターネットを介したコンテンツ視聴時の構成図である。２００ｃはコンテンツ送信装置が一度時間認証した携帯用コンテンツ受信装置である。本来なら、インターネットに接続された携帯用コンテンツ受信装置２００ｃはコンテンツ送信装置１００との時間認証でＴ１＞Ｔとなり認証されず、コンテンツ送信装置１００から送信されるコンテンツを受信できないが、本発明によると、コンテンツ送信装置１００は携帯用コンテンツ受信装置２００ｃを一度時間認証し、携帯用コンテンツ受信装置２００ｃのアドレス情報と装置固有の公開鍵を機器情報登録手段１０８に登録する。これにより、時間認証でＴ１＞Ｔとなる所でも機器情報登録手段１０８に登録されている携帯用コンテンツ受信装置２００ｃは時間認証を行わなくてもコンテンツ送信装置１００から送信されるコンテンツを受信することができる。

【００３１】

また、コンテンツ送信装置１００から送信されるコンテンツを受信し視聴できるのは、機器情報登録手段１０８に登録されている装置のみとなるので、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に制限することができる。

更には認証要求およびその結果に対する認証応答を送信する際のＴＣＰパケットを送信する際やコンテンツの伝送を行うＴＣＰパケットもしくはＵＤＰデータグラムを格納して送信されるＩＰパケットの生存時間ＴＴＬ（Time To Live）を１等の低い値にして送信し、認証要求がルータ４００を通過しないようにしてコンテンツの伝送が個人的な利用の範囲を超えないような制限を加えることもできる。

【実施例４】

【００３２】

以下本発明の実施例４について説明する。

第４の実施の形態は、コンテンツ送信装置５００とコンテンツ受信装置６００において

無線LANを使ってコンテンツの伝送を行うものである。

図８は無線LANを介したコンテンツ送受信装置を示しており、LANとの接続に無線ネットワーク通信処理回路５０３および６０３を用い、WEP（Wired Equivalent Privacy）暗号処理回路５０９および６０９を備えている。WEPは無線LANにおけるセキュリティ保護の目的で標準的に用いられている公知の暗号化方式であり、送信装置と受信装置の間でセキュリティ保護がなされた通信をユーザ管理下で実現することができる。

【００３３】

図９はコンテンツ送信装置５００とコンテンツ受信装置６００を用いた宅内のネットワークの構成の一例を示している。図９においてデータ送信装置５００と２台のデータ受信装置６００ａ、６００ｂが無線アクセスポイント７００により無線ＬＡＮで接続される。無線ＬＡＮアクセスポイント７００はさらにルータ４００に接続され、ルータ４００は図２に示したルータ４００と同様にしてインターネットに接続される。

図８に示すコンテンツ送信装置５００とコンテンツ受信装置６００との間で相互認証とそれに続くコンテンツの伝送を行おうとする場合には、認証回路５０４および６０４によりＷＥＰ暗号処理回路５０９および６０９においてＷＥＰ処理が施されているかどうかをチェックする。そしてＷＥＰ処理が使われていなければ、相互認証とそれに続くコンテンツの伝送を行わないようにするか、もしくは使用者にＷＥＰ処理を起動させるように促す表示を行うなどの必要な処理をおこなうようにする。以上のようにして、無線LANを用いてコンテンツの伝送を行う際には必ずWEP処理が施された状態となるようにする。この結果、コンテンツ送信装置５００およびコンテンツ受信装置６００の使用者が意識しないところで無線LANを介して他のデータ受信装置が接続されてコンテンツの不正なコピーが行われてしまうのを防止する。

【００３４】

上記した以外の点に関しては第１の実施の形態から第３の実施の形態で説明したコンテンツ送信装置およびコンテンツ受信装置により実施されるコンテンツ伝送方法と全く同様にして、コンテンツの不正な複製の作成を抑止して著作権の保護を行うことができ、その際に個人の利用範囲を逸脱したコンテンツの伝送が行なわれないようにすることができる。

【００３５】

図１０は、本発明の実施の形態において、例えばPDA（Personal Digital Assistance）を用いた例について示した図である。（ａ）は、PDA（８００）とコンテンツ送信装置１００、５００との認証時の接続を示しており、（ｂ）は上記認証されたPDA（８００）を用いて、宅外から宅内のコンテンツ送信装置１００、５００のコンテンツを視聴する時の図を示したものである。８００は、コンテンツ送信装置１００、５００から配信されるコンテンツを視聴することができるPDAを、９００は宅内においてコンテンツ送信装置１００、５００が配信するコンテンツを視聴できるディスプレイであり、例えばプラズマディスプレイや液晶ディスプレイである。

【００３６】

例えば、購入してきたPDA（８００）を宅内で接続し、時間認証をコンテンツ送信装置１００とコンテンツ送信装置５００との間で行い、夫々のコンテンツ送信装置１００、５００で認証された場合、コンテンツ送信装置１００、５００はPDA（８００）のアドレス情報と上記時間認証時に使用する機器固有情報である共通鍵を登録し機器を管理することで、従来宅外のPDA（８００）は時間認証により宅内のコンテンツ受信装置１００、５００から配信されるコンテンツの受信を許可されないが、本発明により一度コンテンツ送信装置１００、５００で時間認証を受け機器情報を登録されているので宅内のコンテンツ送信装置１００、５００から配信されるコンテンツを視聴することが出来るようになる。

【実施例５】

【００３７】

以下本発明の実施例５について説明する。

本発明の実施例５では、コンテンツ送信装置１００の機器情報登録回路１０８に登録し

たアドレス情報や機器情報の内容をチェックし、常に最新のネットワーク構成に適した内容に更新する方法について説明する。
図１１は、コンテンツ送信装置１００が保持する機器情報登録手段１０８の構成を示した図である。
機器情報取得部１０８１、機器情報登録部１０８２、機器情報管理部１０８３については、前述と同様である。
機器情報チェック部１０８４は、機器情報登録部１０８２に登録した情報をチェックするために、前記タイマー回路１０７を用いて時間認証を実施し、その測定結果に応じて機器情報管理部１０８３に該登録した情報の内容を更新するように指示する。
【００３８】
図１２は、該機器情報登録部１０８２に登録された情報に対して該機器情報チェック部１０８４が該情報を更新するための管理データの一例を示した図である。
前述したコンテンツ受信装置２００に関する該登録されたアドレス情報や装置固有の機器情報の他に、コンテンツ受信装置２００毎にカウンタ設定値１２０１や現在のカウンタ値１２０２といった管理情報１２００を保持する。
【００３９】
次に、図１３と図１４を用いて、該機器情報チェック部１０８４が機器情報登録部１０８２に登録した情報をチェックする方法について説明する。
図１３は、コンテンツ送信装置１００とコンテンツ受信装置２００の間で認証が成功した場合に、コンテンツ送信装置１００側で実行する手順の一例を示したものである。
コンテンツ受信装置２００との間で認証が成功した場合、コンテンツ送信装置１００は、機器情報登録回路１０８に登録されたアドレス情報と装置固有の機器情報の中に、該コンテンツ受信装置２００のアドレス情報と装置固有の機器情報と一致するものがないか検索する（ステップ１３００）。その結果、一致するものがない場合は、前記認証中に前述した時間認証を行ったか否かを判断し（ステップ１３０１）、時間認証を行っていない場合はタイマー回路１０７を用いて時間認証を実施する（ステップ１３０２）。そして、時間認証の結果を判定し（ステップ１３０３）、成功した場合は、該機器情報登録回路１０８に該コンテンツ受信装置２００のアドレス情報と装置固有の機器情報を登録する（ステップ１３０４）。
【００４０】
その後、該機器情報登録回路１０８内の機器情報チェック部１０８４は、該登録した情報に関する管理情報１２００を作成し、カウンタ設定値１２０１（CountMax）と現在のカウンタ値１２０２（Count）に所定の値（Ｐ１）を設定する（ステップ１３０５）。そして、該タイマー回路１０７をスタートさせ、所定の時間（Ｔ４）が経過する毎にイベント通知するように設定し（ステップ１３０６）、ネットワーク上の装置からの通信や認証要求の待ち状態にする（ステップ１３０７）。
ここで、ステップ１３０３において時間認証に失敗した場合は、必要であれば時間認証をリトライし、なおも失敗する場合には該コンテンツ受信装置２００に対してコンテンツを送信しない状態にして処理を終了する。
【００４１】
また、ステップ１３００において該コンテンツ受信装置２００が既に登録済みの場合は、ステップ１３０５の処理に移る。あるいは、管理情報１２００内のカウンタ設定値１２０１（CountMax）と現在のカウンタ値１２０２（Count）を参照し、Count＜CountMaxで該タイマー回路１０７が既に動作中の場合はステップ１３０７の処理に移っても良い。
また、ステップ１３０５においてカウンタ設定値１２０１（CountMax）に設定する所定の値（Ｐ１）は、全コンテンツ受信装置に共通した値でもコンテンツ受信装置毎に異なっても良い。
【００４２】
次に図１４は、上記ステップ１３０７の通知待ち状態で所定の時間（Ｔ４）が経過して該タイマー回路１０７によりイベント通知が発生した場合に、コンテンツ送信装置１００

側で実行する手順の一例を示したものである。
まず、時間Ｔ４が経過すると前記タイマー回路１０７はタイマーイベントを発生させ、コンテンツ送信装置１００に通知する（ステップ１４００）。これを受けて、該機器情報チェック部１０８４は、現在のカウンタ値１２０２（Ｃｏｕｎｔ）の値をデクリメントし（ステップ１４０１）、Ｃｏｕｎｔ＝０になったか否かを判定する（ステップ１４０２）。

【００４３】

その結果、Ｃｏｕｎｔ＝０になった場合には、この時点で、前記機器情報登録回路１０８に登録した前記コンテンツ受信装置２００に関する情報や、必要であれば認証鍵、交換鍵、共通鍵を破棄する方法もあるが、本発明の実施の形態では、再度該タイマー回路１０７を用いて該コンテンツ受信装置２００との間で時間認証を実施する（ステップ１４０３）。そして、時間認証の結果を判定し（ステップ１４０４）、成功した場合は、管理情報１２００内の現在のカウンタ値１２０２にカウンタ設定値１２０１の値を設定（Ｃｏｕｎｔ＝ＣｏｕｎｔＭａｘ）し（ステップ１４０７）、前述同様に該タイマー回路１０７をスタートさせ（ステップ１４０８）要求待ち状態にする（ステップ１３０７）。一方、ステップ１４０４において時間認証に失敗した場合は、必要であれば時間認証をリトライし、なおも失敗する場合には、該機器情報チェック部１０８４は該機器情報管理部１０８３に対して前記コンテンツ受信装置２００に関する情報を削除するように要求し、必要であれば認証鍵、交換鍵、共通鍵も破棄する（ステップ１４０５）。そして最後に要求待ち状態にする（ステップ１３０７）。

【００４４】

一方、ステップ１４０２において、Ｃｏｕｎｔ＞０である場合には、再度該タイマー回路１０７をスタートさせて所定の時間（Ｔ４）が経過する毎にイベント通知するように設定し（ステップ１４０８）、要求待ち状態に戻る（ステップ１３０７）。
ここで、上記では、前記機器情報登録回路１０８にコンテンツ受信装置２００に関する情報を登録した後、該機器情報チェック部１０８４が現在のカウンタ設定値１２０２をデクリメントするタイミングとして、一定の時間（Ｔ４）を使用し、所定の時間（Ｔ４×CountMax）が経過する毎に時間認証を行っているが、コンテンツを送信していない時間（あるいは送信している時間）を計測し、その累積値が一定の時間（Ｔ５）に達した場合に行うことも可能である。

【００４５】

また、上記では、カウンタ設定値を更新するタイミングとして時間（Ｔ４／Ｔ５）を用いたが、コンテンツ受信装置２００に対して送信したコンテンツの所定のパケット数、あるいはコンテンツ送信時に行う共通鍵の所定の更新回数などを用いることも可能である。
また、前記機器情報登録回路１０８にコンテンツ受信装置２００に関する情報を登録した後、該コンテンツ受信装置２００がネットワーク上に存在しているか否かを常に監視し、存在していないことを検知した時点で、カウンタ設定値１２０１、現在のカウンタ設定値１２０２を設定し、該タイマー回路１０７をスタートさせて定期的に時間計測を行って現在のカウンタ設定値１２０２を更新し、ネットワーク上に存在していない時間が所定の時間に達すると、該機器情報登録回路１０８から該受信装置２００に関する情報を削除し、必要であれば認証鍵、交換鍵、共通鍵も破棄することも可能である。ネットワーク上に装置が存在するか否かの監視方法については、特定のものに限定されることはなく、ＴＣＰが提供するキープアライブ機能等を用いることができる。

【００４６】

さらには、該機器情報チェック部１０８４に複数のカウンタ（CountMax１、Ｃｏｕｎｔ１、CountMax２、Ｃｏｕｎｔ２）を持たせ,時間認証を行うタイミングを複数組み合わせることも可能である。例えば、現在のカウンタ設定値Ｃｏｕｎｔ１は時間（Ｔ４）毎にデクリメントし、現在のカウンタ設定値Ｃｏｕｎｔ２は送信パケット数（Ｐ１）毎にデクリメントし、どちらか一方が所定の値（CountMax１、CountMax２）に到達した場合に時間認証を行うなどが想定される。

【００４７】

ここで、上記ではコンテンツ送信装置１００について記述したが、コンテンツ送信装置５００、コンテンツ受信装置２００、６００に対しても同様に適用できる。
以上のことから、コンテンツ送信装置およびコンテンツ受信装置の機器情報チェック部１８０４が、機器情報登録回路１０８に登録したコンテンツ受信装置２００に関する情報について定期的に時間認証を行うことにより、未接続の装置や使用頻度の低い装置に関する登録情報が該機器情報登録回路１０８に登録されたままになることを防ぎ、ネットワーク構成に応じた適切な登録情報の管理が可能となる。

【実施例６】

【００４８】

以下本発明の実施例６について説明する。

前述の実施例５では、コンテンツ送信装置１００の機器情報チェック部１８０４が、機器情報登録回路１０８に登録したコンテンツ受信装置２００に対して定期的に時間認証を行う方法について記述したが、本発明の実施例６では、コンテンツ送信装置１００が必要時に任意のタイミングで時間認証を行う方法について説明する。
ここで、必要時とは、例えば、コンテンツ送信装置１００の電源やネットワークが切断あるいはスタンバイ状態になり、再度電源が投入あるいはネットワークに接続した場合が挙げられる。また、コンテンツ送信装置１００とコンテンツ受信装置２００との間で予約視聴や予約録画など、実行中にコンテンツの転送が中断しては困るような処理を行う場合が挙げられる。

【００４９】

図１５は、コンテンツ送信装置１００の電源が切れたあるいはスタンバイ状態になった後、再度電源が投入された場合に、コンテンツ送信装置１００側で実行する一連の処理手順の一例を示したものである。
最初に、コンテンツ送信装置１００は、電源投入時に必要なシステムの設定、初期化処理を行い（ステップ１５００）、ネットワーク上に存在する装置の検出を行う（ステップ１５０１）。装置の検出方法については特定のものに限定されることはなく、ＵＰｎＰ（Universal Plug and Play）、Ｊｉｎｉ等を用いることができる。
次に、機器情報登録回路１０８にアドレス情報と装置固有の機器情報が登録されているか否かを判定し（ステップ１５０２）、１台以上のコンテンツ受信装置２００について登録されている場合には、コンテンツ受信装置２００に対してタイマー回路１０７を用いて時間認証を実施する（ステップ１５０３）。そして、時間認証の結果を判定し（ステップ１５０４）、成功した場合は、前記機器情報チェック部１８０４が管理する管理情報１２００内の現在のカウンタ値１２０２にカウンタ設定値１２０１の値を設定（Ｃｏｕｎｔ＝ＣｏｕｎｔＭａｘ）し（ステップ１５０５）、前述同様に該タイマー回路１０７をスタートさせる（ステップ１５０７）。

【００５０】

一方、ステップ１５０４において失敗した場合は、必要であれば時間認証をリトライし、なおも失敗する場合には機器情報登録回路１０８内の該コンテンツ受信装置２００に関する登録情報を削除する（ステップ１５０６）。
そして、登録された全てのコンテンツ受信装置２００に対して時間認証が終了した場合（ステップ１５０８）には、ネットワーク上の装置からの通信や認証要求の待ち状態にする（ステップ１３０８）。

【００５１】

ここで、ステップ１５０１、１５０２において、現在ネットワーク上に存在する装置と機器情報登録回路１０８に登録されているアドレス情報と装置固有の機器情報とを比較し、アドレス情報と装置固有の機器情報は存在するがネットワーク上に存在しない装置に関しては、その時点でアドレス情報と装置固有の機器情報を削除することも可能である。
また、ステップ１５０５、１５０６において、時間認証成功後に該タイマー回路１０７をスタートさせているが、ステップ１５０８の後に行っても良い。

【００５２】

以上のことから、コンテンツ送信装置１００の電源やネットワークが切断あるいはスタンバイ状態になり、再度電源が投入あるいはネットワークに接続した場合に、登録しているコンテンツ受信装置２００に対して時間認証を行うことにより、登録情報を最新のネットワーク構成を考慮した内容に更新することが可能となる。

【００５３】

次に、図１６は、コンテンツ送信装置１００が送信するコンテンツをコンテンツ受信装置２００で予約録画を行う場合に、コンテンツ送信装置１００側で実行する手順の一例を示したものである。

まず、コンテンツ送信装置１００は、予約録画を開始する前に、コンテンツ送信先であるコンテンツ受信装置２００を特定し（ステップ１６００）、該コンテンツ受信装置２００のアドレス情報や装置固有の機器情報が機器情報登録回路１０８に登録されているか否かを判定する（ステップ１６０１）。その結果、既に登録済みである場合にはタイマー回路１０７を用いてコンテンツ受信装置２００に対して時間認証を行い（ステップ１６０２）、その結果を判定する（ステップ１６０３）。時間認証に成功した場合は、前記機器情報チェック部１８０４が管理する管理情報１２００内の現在のカウンタ値１２０２にカウンタ設定値１２０１の値を設定（Ｃｏｕｎｔ＝ＣｏｕｎｔＭａｘ）し（ステップ１６０４）、前述同様に該タイマー回路１０７をスタートさせる（ステップ１６０５）。その後、該コンテンツ受信装置２００からコンテンツ要求を受信するとコンテンツの送信を開始する（ステップ１６０６）。

【００５４】

ここで、ステップ１６０１において、該コンテンツ受信装置２００が登録されていない場合は、該コンテンツ受信装置２００からの認証要求待ちになる（ステップ１３０７）。ここで、上記一連の手順は、予約視聴や予約実行以外に、コンテンツ送信装置１００が送信中のコンテンツの種別が変化した場合（例えば、放送番組の切替り時や選局時、蓄積番組の変更時など）にも同様の手順を行うことが可能である。また、該コンテンツ受信装置２００の動作状態を常に監視し、電源やネットワークが一旦切断されたコンテンツ受信装置２００を再度その存在を検知した場合や録画状態を検知した場合などにも同様の手順を行うことが可能である。

【００５５】

以上のことから、予約視聴や予約録画などを実行する前にコンテンツ受信装置２００との間で予め時間認証を行い、現在のカウンタ値１２０２（Ｃｏｕｎｔ）をカウンタ設定値（ＣｏｕｎｔＭａｘ）に戻すことにより、予約視聴中や予約録画中に時間認証が動作することを極力避けることができ、また該コンテンツ受信装置２００に関する登録情報を削除したりコンテンツ伝送を中断するといった事態を避けることが可能となる。

【実施例７】

【００５６】

以下本発明の実施例７について説明する。

本発明の実施例７では、コンテンツ送信装置１００の機器情報チェック部１８０４が管理するカウンタ値（Count）をコンテンツ受信装置２００側から任意のタイミングで更新する方法について説明する。

図１７は、コンテンツ送信装置１００とコンテンツ受信装置２００との間で時間認証を実行する手順の一例を示したものである。左側がコンテンツ送信装置１００を、右側がコンテンツ受信装置２００を表しており、時間認証においける所定の値については図６に示した時間（Ｔ３）を用いる。

【００５７】

前述の通り、コンテンツ受信装置２００からコンテンツ送信装置１００に対して認証要求が発行されると、一連の認証処理が開始する。そして、時間認証を実行して成功した場合に、コンテンツ送信装置１００は、機器情報登録回路１０８に該コンテンツ受信装置２００に関するアドレス情報や装置固有の機器情報を登録し、機器情報チェック部１８０４は前述同様に現在のカウンタ値（Count）にカウンタ設定値（CountMax）の値を設定し、

該タイマー回路１０７をスタートさせて、該コンテンツ受信装置２００やネットワーク上の他の装置からの要求受信待ち状態になる。
ここで、本実施例では、該コンテンツ送信装置１００は現在のカウンタ値Count＝０に達した場合は、機器情報登録回路１０８に登録した該コンテンツ受信装置２００に関する情報を削除するものとする。

【００５８】

このような状況下で、該コンテンツ受信装置２００は、コンテンツ１の送信要求を作成して該コンテンツ送信装置１００に対して送信すると、該コンテンツ送信装置１００は、該コンテンツ１を暗号化して送信する。該コンテンツ１の受信を完了した後、さらに該コンテンツ受信装置２００がコンテンツ２を受信したい場合は、時間認証の実行要求を作成して該コンテンツ送信装置１００に対して送信する。該要求を受信した該コンテンツ送信装置１００は、該タイマー回路１０７を用いて時間認証を実行し、成功した場合は、該現在のカウンタ値（Ｃｏｕｎｔ）を再度カウンタ設定値（CountMax）に設定する。その後、該コンテンツ受信装置２００はコンテンツ２の送信要求を作成して該コンテンツ送信装置１００に対して送信する。

【００５９】

上記では、コンテンツ受信装置２００がコンテンツ１の受信とコンテンツ２の受信との間に時間認証の実行要求を送信しているが、定期的にあるいは／さらに任意のタイミング（例えば、予約視聴・予約録画前、電源投入時など）で行うことも可能である。
また、コンテンツ受信装置２００がコンテンツ送信装置１００に対して現在のカウンタ値（Ｃｏｕｎｔ）を問い合わせし、該カウンタ値が所定の閾値以下になると、時間認証の実行要求を送信する方法もある。

【００６０】

以上のことから、コンテンツ受信装置２００がコンテンツ送信装置１００に対して時間認証の実行要求を送信し、時間認証を実行することにより、コンテンツ送信装置１００側の該受信装置２００に関する登録情報が削除されないように制御することが可能となる。

【００６１】

以上、本発明の実施の形態について、コンテンツ送信装置がコンテンツ受信装置を認証要求に対する認証を行い、コンテンツ受信装置のアドレス情報と機器の固有情報を登録することで、有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用の範囲に制限することのできるコンテンツ送信装置、受信装置を提供することができることを説明してきたが、コンテンツ受信装置がコンテンツ送信装置を認証して該コンテンツ送信装置のアドレス情報と機器の固有情報を登録することで、上記同様の効果を得られることは言うまでもない。また、以上の説明ではネットワークを介して伝送する対象を映像情報等のコンテンツとし、コンテンツを送受信するコンテンツ送信装置、受信装置として説明したが、映像情報等以外の種類の情報についても同様であり、これらの情報を入出力する情報処理装置についても、本発明を実施できることは言うまでもない。

さらに、コンテンツ送信装置とコンテンツ受信装置との間で定期的にあるいは適宜時間認証を実施することにより、上記アドレス情報や機器の固有情報などの登録内容を動的に管理することができる。

【産業上の利用可能性】

【００６２】

宅内の有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成が個人的利用利用の範囲に制限することのできるコンテンツ送信装置、受信装置を提供することができる。

【図面の簡単な説明】

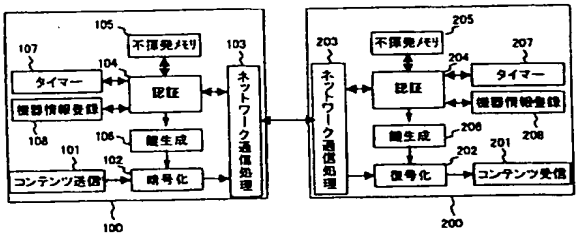
【００６３】

【図１】本発明のコンテンツ送信装置、コンテンツ受信装置の有線LANを用いた構成を示す図。
【図２】本発明のコンテンツ送信装置、コンテンツ受信装置で構成される有線LANのブロック図。
【図３】本発明のコンテンツ送信装置の機器情報登録回路の詳細図。
【図４】本発明のコンテンツ送信装置の機器情報登録回路に登録されるリストを示す図。
【図５】本発明のコンテンツ受信装置とコンテンツ受信装置間でコンテンツの伝送を行う手順を示した図。
【図６】本発明のコンテンツ受信装置とコンテンツ受信装置間でセキュアでかつ正確な時間認証を行なう手順を示した図。
【図７】本発明のコンテンツ送信装置、コンテンツ受信装置でインターネットを介したコンテンツ送受信時の構成を示した図。
【図８】本発明のコンテンツ送信装置、コンテンツ受信装置の無線LANを用いた構成を示す図。
【図９】本発明のコンテンツ送信装置、コンテンツ受信装置で構成される無線LANのブロック図。
【図１０】本発明におけるPDAを用いた場合の構成例を示す図。
【図１１】本発明のコンテンツ送信装置の機器情報登録回路の詳細図の一例。
【図１２】本発明のコンテンツ送信装置の機器情報登録回路に登録されるリストを示す図の一例。
【図１３】本発明のコンテンツ送信装置とコンテンツ受信装置の間で認証が成功した場合に、コンテンツ送信装置側で実行する手順の一例。
【図１４】本発明のコンテンツ送信装置が定期的に時間認証を実行する手順の一例。
【図１５】本発明のコンテンツ送信装置の電源を投入する際に、コンテンツ送信装置が時間認証を実行する手順の一例。
【図１６】本発明のコンテンツ送信装置とコンテンツ受信装置の間で予約視聴あるいは予約録画を実行する際に、コンテンツ送信装置が時間認証を実行する手順の一例。
【図１７】本発明のコンテンツ受信装置が時間認証を要求する手順の一例。
【符号の説明】
【００６４】
１００、５００ …コンテンツ送信装置
１０１、５０１ …コンテンツ送信回路
１０２、５０２ …暗号化回路
１０３、５０３ …ネットワーク通信処理回路
１０４、５０４ …認証回路
１０５、５０５ …不揮発メモリ
１０６、５０６ …鍵生成回路
１０７、５０７ …タイマー回路
１０８、５０８ …機器情報登録回路
２００、６００ …コンテンツ受信装置
２０１、６０１ …コンテンツ受信回路
２０２、６０２ …暗号化回路
２０３、６０３ …ネットワーク通信処理回路
２０４、６０４ …認証回路
２０５、６０５ …不揮発メモリ
２０６、６０６ …鍵生成回路
２０７、６０７ …タイマー回路
２０８、６０８ …機器情報登録回路
３００ …ハブ
４００ …ルータ

７００ …無線アクセスポイント
８００ …PDA
９００ …ディスプレイ

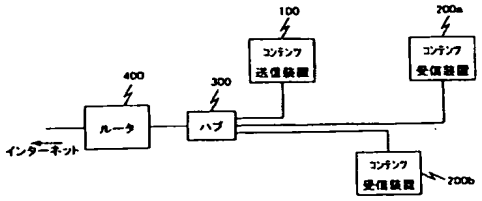
【図１】

図 1



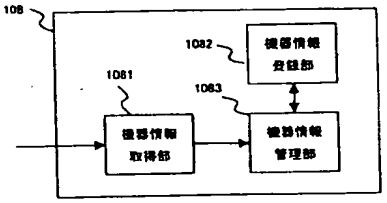
【図２】

図 2



【図３】

図 3



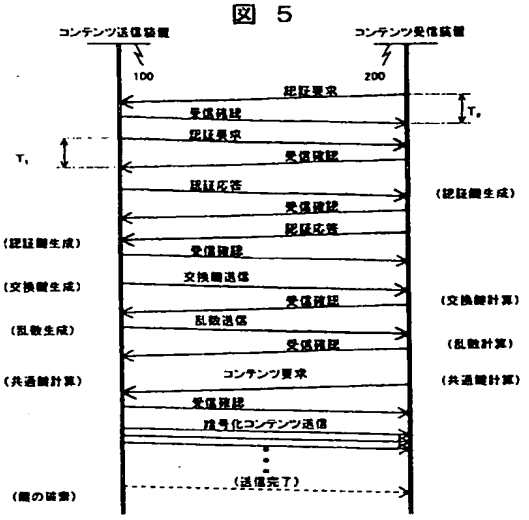
【図４】

図 4

アドレス情報		装置固有情報
IP	MAC	公開鍵
aaa.aaa.aaa.aaa	aa:bb:cc:dd:ee:ff	abcdefg……
bbb.bbb.bbb.bbb	bb:cc:dd:ee:ff:aa	bcdefgh……

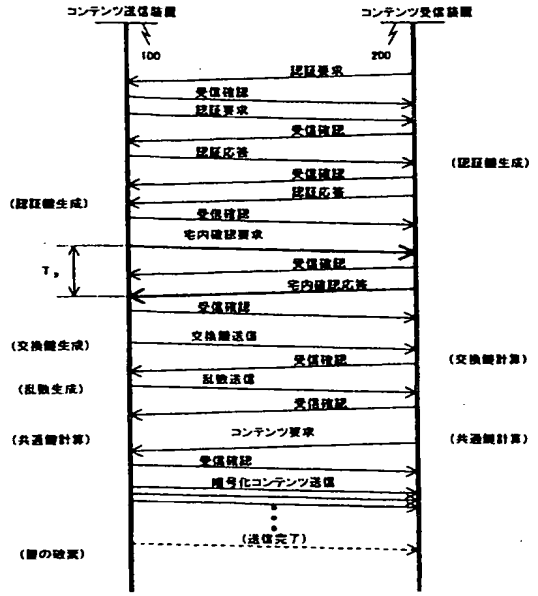
【図５】

図 5



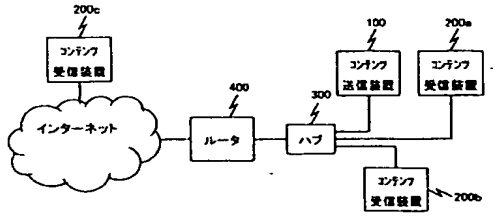
【図６】

図 6



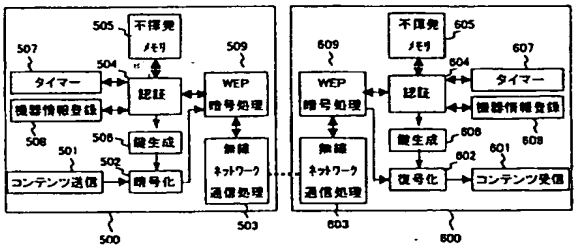
【図７】

図 7



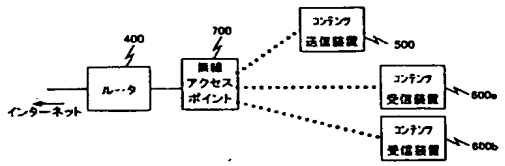
【図８】

図 8



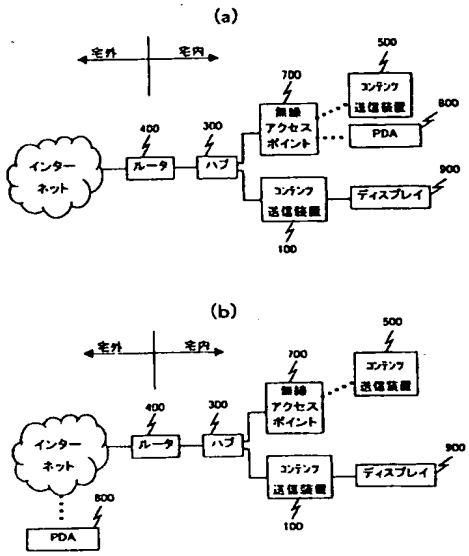
【図９】

図 9



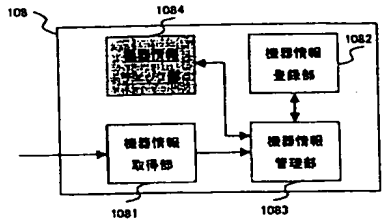
【図１０】

図 10



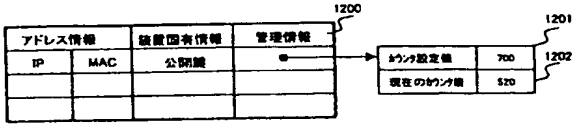
【図１１】

図11



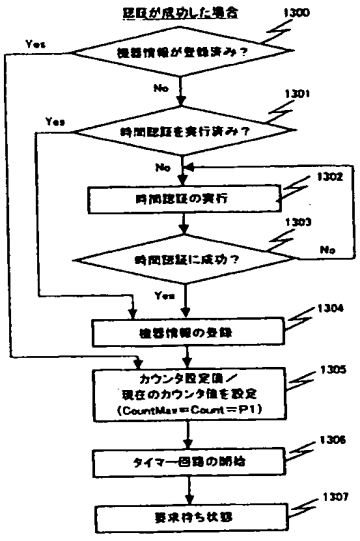
【図１２】

図12



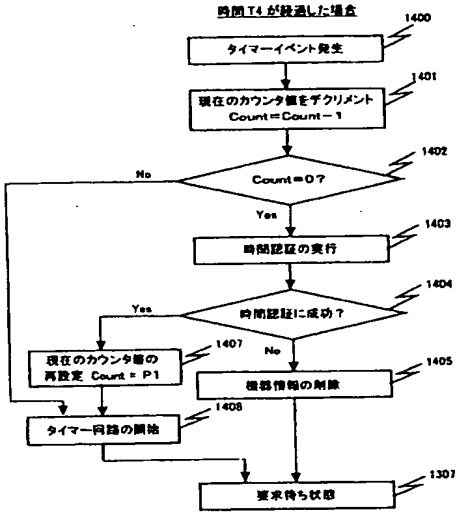
【図１３】

図13



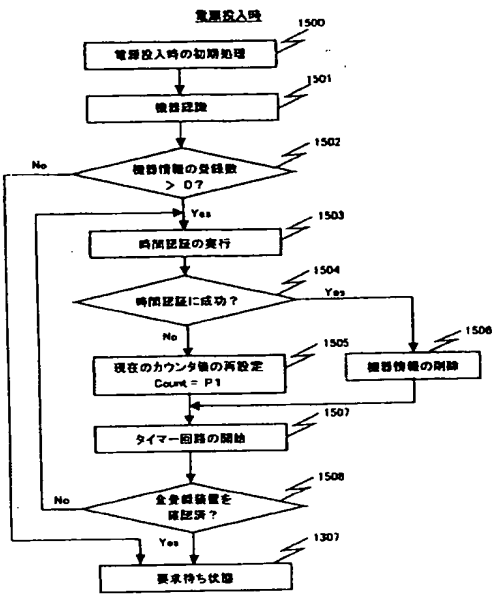
【図１４】

図14



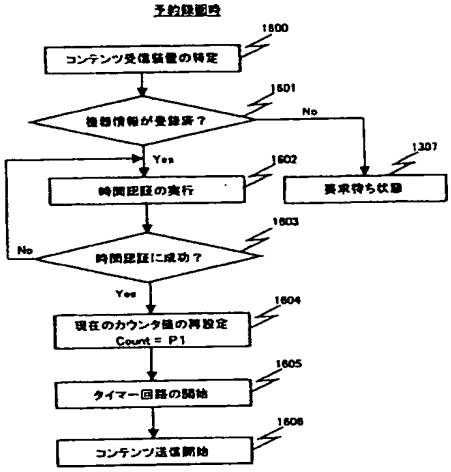
【図１５】

図15



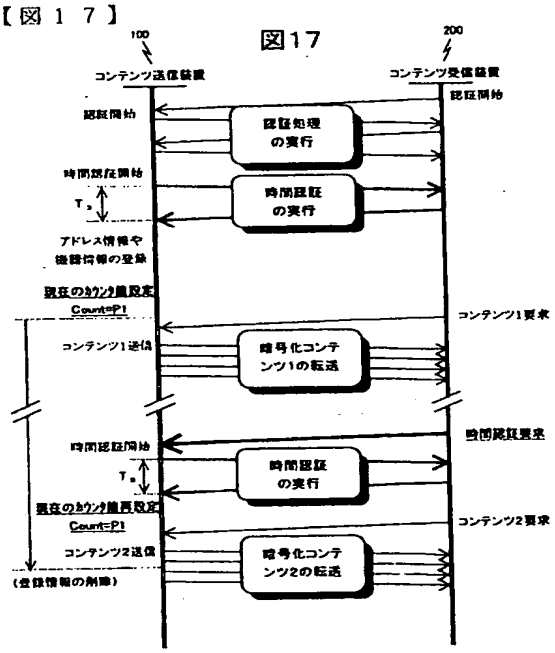
【図１６】

図16



【図１７】

図17



フロントページの続き

Fターム(参考) 5B085 AA08 AE04
5J104 AA07 EA23 KA02 KA04 PA07